Journal of Information and Information Security (JIFORTY)
Vol. 2, No. 1, Juni 2021, 177-186
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Analisis Keamanan Aplikasi Fintech di Indonesia: Studi Kasus OVO, GoPay, ShopeePay dan Dana

Bertnardo Mario Uskono[1,*], Rian Wijaya [1], Mochamad Galih Pradipta [1], Aldiansyah Kusnadi [1]

[1] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Perjuangan No.81, Marga Mulya, Kec. Bekasi Utara, Kota Bekasi, Jawa Barat 17143; e-mail: 202210715326@mhs.ubharajaya.ac.id, 202210715308@mhs.ubharajaya.ac.id, 202210715322@mhs.ubharajaya.ac.id, 202210715111@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715326@mhs.ubharajaya.ac.id

Diterima: 4 Jan 25; Review: 4 Jan 25; Disetujui: 8 Jan 25; Diterbitkan: 8 Jan 25

Abstract

This research analyzed the security of four leading digital wallet applications in Indonesia (OVO, GoPay, ShopeePay, and DANA) using the Mobile Security Framework (MobSF) to identify potential user data security vulnerabilities. Through static analysis methods, the study examined security parameters such as weak encryption, SSL bypass, dangerous permissions, and hidden secret detection, aiming to provide a comprehensive insight into fintech data protection. Research findings revealed that all four applications were at security level four, with security scores ranging from 45-48, which highlighted significant security improvements for ShopeePay and DANA from the previous year, while OVO and GoPay showed minimal changes, underscoring the importance of continuous enhancement in digital financial application security.
***Keywords**: fintech security, digital wallet, MobSF, security analysis, data protection*

Abstrak

Penelitian ini menganalisis keamanan empat aplikasi dompet digital terkemuka di Indonesia (OVO, GoPay, ShopeePay, dan DANA) menggunakan Mobile Security Framework (MobSF) untuk mengidentifikasi potensi kerentanan keamanan data pengguna. Melalui metode analisis statis, penelitian mengkaji parameter keamanan seperti enkripsi lemah, bypass SSL, izin berbahaya, dan deteksi rahasia tersembunyi, dengan tujuan memberikan wawasan komprehensif tentang perlindungan data fintech. Hasil penelitian menunjukkan bahwa keempat aplikasi berada pada tingkat keamanan empat, dengan skor keamanan bervariasi antara 45-48, yang mengungkapkan peningkatan signifikan keamanan ShopeePay dan DANA dari tahun sebelumnya, sementara OVO dan GoPay menunjukkan perubahan minimal, yang menyoroti pentingnya peningkatan berkelanjutan dalam keamanan aplikasi keuangan digital.
Kata kunci: keamanan fintech, dompet digital, MobSF, analisis keamanan, perlindungan data

1. Pendahuluan

Pada era digital ini, penggunaan teknologi finansial atau financial technology (fintech) semakin luas dan masif, menghadirkan inovasi dalam transaksi keuangan melalui aplikasi-aplikasi digital. Hal ini terasa dari beberapa kebijakan pemerintah yang mendorong masyarakatnya menggunakan teknologi, mulai dari sektor pendidikan, bisnis, transportasi dan lainnya. Bahkan fenomena politik tak lepas dari keterkaitan teknologi informasi. Masyarakat

tingkat menengah-bawah pun harus siap dengan perkembangan yang begitu pesat (Wijayanto et al., 2020). Fintech, menurut definisi dari Bank Indonesia dalam Pasal 1 Angka 1 Peraturan Bank Indonesia Nomor 19/12/PBI/2017, adalah pemanfaatan teknologi dalam sistem keuangan yang menciptakan produk dan layanan keuangan yang dapat memengaruhi stabilitas moneter serta efisiensi, keamanan, dan keandalan sistem pembayaran(Peraturan Bank Indonesia Nomor 19/12/PBI/2017, 2017). Secara global, Financial Stability Board mendefinisikan fintech sebagai inovasi teknologi dalam layanan keuangan yang menghasilkan berbagai model bisnis, aplikasi, dan produk baru yang berdampak pada penyediaan layanan keuangan (Jelamu et al., 2024).

Salah satu produk fintech yang populer di Indonesia adalah dompet digital atau e-wallet. Beberapa aplikasi e-wallet terkemuka, seperti GoPay, OVO, DANA, dan ShopeePay, menawarkan kemudahan dan kepraktisan dalam bertransaksi secara digital, baik online maupun offline(Marginingsih, 2021) . E-wallet ini memungkinkan transaksi yang cepat dan efisien, sehingga menarik banyak pengguna dari berbagai kalangan, termasuk mereka yang kurang familiar dengan teknologi keuangan. Namun, dengan meningkatnya jumlah pengguna, risiko keamanan data pengguna juga semakin besar. Kejahatan siber, seperti pencurian data dan penipuan digital, menjadi ancaman yang serius dan harus diantisipasi. Oleh karena itu, pengujian keamanan aplikasi menjadi sangat penting untuk menjaga privasi dan data pengguna.(Firmansyah et al., 2024)

Dalam penelitian ini, Mobile Security Framework (MobSF) akan digunakan sebagai alat untuk menganalisis keamanan pada aplikasi-aplikasi e-wallet. MobSF adalah aplikasi yang dirancang untuk menganalisis keamanan paket aplikasi Android, khususnya yang berformat APK. Aplikasi ini menyediakan laporan analisis yang cepat, efisien, dan mendalam, serta dapat diakses secara bebas dan online (Munir & Hakim, 2024). Melalui MobSF, penelitian ini akan mengidentifikasi potensi kerentanan dan risiko keamanan pada aplikasi e-wallet GoPay, OVO, ShopeePay dan DANA, dengan tujuan meningkatkan perlindungan terhadap data pengguna dan memastikan keamanan dalam bertransaksi.(Riset et al., 2024)

Dengan demikian, penelitian ini diharapkan dapat memberikan wawasan mendalam terkait keamanan aplikasi e-wallet di Indonesia dan mendorong penyedia layanan untuk terus meningkatkan proteksi terhadap data dan privasi pengguna, sehingga pengguna dapat bertransaksi dengan aman dan nyaman.

2. Metode Penelitian

2.1 Metode Pengumpulan Data

2.1.1 Studi Pustaka.

Peneliti mencari dan membaca berbagai sumber informasi yang berhubungan dengan keamanan data pengguna di aplikasi fintech. Sumber-sumber ini diambil dari buku, artikel, jurnal, dan dokumen online seperti yang ada di Google Scholar. Tujuannya adalah untuk memahami konsep dasar dan mendapatkan referensi yang relevan dengan penelitian ini.

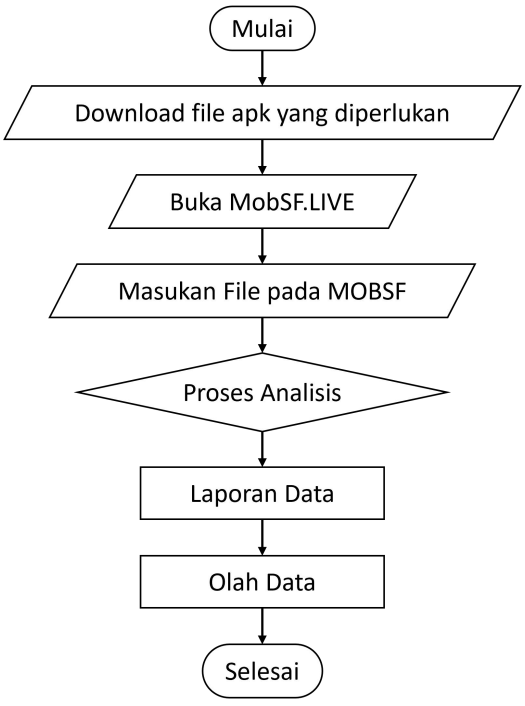
2.1.2 Pengamatan.

Peneliti melakukan pengamatan langsung dengan menggunakan Mobile Security Framework (MobSF) untuk menganalisis keamanan aplikasi GoPay, OVO, DANA, dan ShopeePay. Proses ini melibatkan pemindaian aplikasi untuk mencari potensi masalah keamanan seperti data yang tidak terenkripsi dengan baik atau izin yang tidak sesuai. Hasil dari pemindaian ini kemudian dianalisis lebih lanjut untuk melihat tingkat keamanan aplikasi tersebut.

2.2 Metode Analisis

Analisis pada aplikasi dilakukan menggunakan metode statis, yang dimana metode statis adalah metode penganalisisan terhadap kode suatu aplikasi. Pada tahap ini perangkat lunak yang digunakan untuk melakukan analisis adalah MOBSF. Analisis metode statis yang dilakukan meliputi:

- Analisis metode enkripsi (SSL bypass)
- Analisis Kelemahan kriptografi (Weak Crypto)
- Analisis hak akses aplikasi (Permissions)
- Analisis sisipan kode berbahaya (Hardcode secrets)
- Analisis malware (Malware check) (Yasa & Nugraha, 2024)



Sumber: Hasil Penelitian (2024)

Gambar 1. Alur Kerja Analisis Statis.

Pada Gambar 1 menunjukan ditampilkan alur kerja proses analisis keamanan aplikasi menggunakan Mobile Security Framework (MobSF). Proses dimulai dengan mengunduh file APK yang diperlukan untuk analisis, kemudian membuka platform MobSF.LIVE sebagai alat utama. File APK tersebut dimasukkan ke dalam MobSF, di mana selanjutnya dilakukan proses

analisis untuk mengevaluasi aspek keamanan aplikasi. Setelah analisis selesai, MobSF menghasilkan laporan data yang berisi hasil evaluasi keamanan. Data dari laporan tersebut kemudian diolah lebih lanjut untuk keperluan tertentu, sebelum proses diakhiri dengan tahap selesai. Alur ini dirancang untuk memastikan setiap tahapan analisis berjalan secara sistematis dan efisien.

3. Hasil dan Pembahasan

3.1. Analisis

Tingkat keamanan aplikasi dapat diukur berdasarkan beberapa parameter seperti *weak crypto*, *SSL bypass*, *dangerous permission*, *hardcode secret*, *root detection*, dan pemeriksaan malware. Analisis keamanan ini dilakukan untuk memberikan skor keamanan dari setiap aplikasi berdasarkan tingkat perlindungan yang diterapkan(Rizkika et al., 2024).

Tingkat keamanan dapat dibagi menjadi empat tingkatan :

1. Tingkat Nol: Merupakan keamanan fisik yang menjaga perangkat keras dan sistem dasar aplikasi.
2. Tingkat Satu: Meliputi keamanan informasi dasar seperti desain basis data, keamanan perangkat, dan pengelolaan akses data.
3. Tingkat Dua: Menyediakan keamanan jaringan untuk mencegah serangan eksternal melalui koneksi jaringan.
4. Tingkat Tiga: Berfokus pada perlindungan informasi lebih kompleks melalui teknologi keamanan canggih.
5. Tingkat Empat: Semua perlindungan tingkat satu sampai tingkat tiga. Jika salah satu tindakan perlindungan tidak terpenuhi, tingkat keamanan empat juga tidak terpenuhi.(Sulomo, 2019)

Analisis dilakukan dengan menggunakan metode statis, pada analisis kali ini dibantu dengan aplikasi MobSF. Hasil analisis dapat dilihat melalui tabel 1 dibawah ini:

Tabel 1. Hasil Analisis Statis

Hasil Analisis Statis Aplikasi Dompet Digital								
NO	Nama Aplikasi	Weak Crypto	SSL Bypass	Dangerous Permission	Harcode Secret	Root Detections	Malware Check	Security Score
1	OVO	YES	YES	YES	NO	YES	GOOD	48
2	GoPay	YES	YES	NO	NO	YES	GOOD	47
3	Shopee Pay	YES	YES	YES	YES	YES	GOOD	45
4	DANA	YES	YES	NO	YES	YES	GOOD	45

Sumber: Hasil Penelitian (2024)

Pada tabel 1 menjelaskan hasil analisis keamanan menggunakan Mobile Security Framework (MobSF) pada empat aplikasi dompet digital, tingkat keamanan dan peringkat aplikasi adalah sebagai berikut:

1. OVO
    - Keamanan: Tingkat 4
    - Parameter: Weak Crypto (Yes), SSL Bypass (Yes), Dangerous Permission (Yes), Hardcode Secret (No), Root Detection (Yes), Malware Check (Good)
    - Skor Keamanan: 48
    - Peringkat: 1
2. GoPay
    - Keamanan: Tingkat 4
    - Parameter: Weak Crypto (Yes), SSL Bypass (Yes), Dangerous Permission (No), Hardcode Secret (No), Root Detection (Yes), Malware Check (Good)
    - Skor Keamanan: 47
    - Peringkat: 2
3. ShopeePay
    - Keamanan: Tingkat 4
    - Parameter: Weak Crypto (Yes), SSL Bypass (Yes), Dangerous Permission (Yes), Hardcode Secret (Yes), Root Detection (Yes), Malware Check (Good)
    - Skor Keamanan: 45
    - Peringkat: 3
4. DANA
    - Keamanan: Tingkat 4
    - Parameter: Weak Crypto (Yes), SSL Bypass (Yes), Dangerous Permission (No), Hardcode Secret (Yes), Root Detection (Yes), Malware Check (Good)
    - Skor Keamanan: 45
    - Peringkat: 3

Hasil ini menunjukkan bahwa seluruh aplikasi yang dianalisis memiliki tingkat keamanan pada level empat, yang menandakan bahwa setiap aplikasi telah memenuhi sebagian besar indikator perlindungan dasar dalam memastikan keamanan pengguna. Meski demikian, perbedaan skor keamanan di antara aplikasi tersebut mencerminkan adanya variasi

dalam jumlah risiko spesifik yang ditemukan selama proses pengujian. Perbedaan ini dapat disebabkan oleh perbedaan pendekatan setiap penyedia layanan dalam menangani aspek-aspek keamanan tertentu, seperti penerapan enkripsi yang lebih kuat, mekanisme deteksi root yang lebih andal, atau pengelolaan izin yang lebih hati-hati. Skor yang lebih rendah pada beberapa aplikasi, meskipun tetap berada pada tingkat keamanan yang sama, menunjukkan bahwa masih terdapat kerentanan atau potensi risiko yang memerlukan perhatian lebih lanjut. Hal ini menyoroti pentingnya upaya berkelanjutan dalam meningkatkan keamanan, terutama mengingat semakin kompleksnya ancaman siber di era digital. Dengan demikian, penyedia layanan dompet digital perlu terus berinovasi dan memperbarui teknologi serta kebijakan keamanannya untuk mengurangi risiko, meningkatkan kepercayaan pengguna, dan memastikan perlindungan data yang optimal.

3.2. Perbandingan Hasil Penelitian

Setelah menyelesaikan analisis mendalam terhadap keamanan masing-masing aplikasi dompet digital, langkah penting berikutnya adalah membandingkan hasil yang diperoleh dengan temuan dari penelitian serupa pada tahun 2023. Perbandingan ini bertujuan untuk mengidentifikasi sejauh mana peningkatan keamanan telah dicapai oleh masing-masing aplikasi, serta memahami tren atau perubahan signifikan yang terjadi dalam perlindungan data pengguna. Berikut adalah hasil analisis keamanan aplikasi dompet digital pada tahun 2023 yang akan menjadi dasar perbandingan dalam penelitian ini:

Tabel 2. Hasil analisis statis pada tahun 2023

Hasil Analisis Statis Aplikasi Dompet Digital								
NO	Nama Aplikasi	Weak Crypto	SSL Bypass	Dangerous Permission	Harcode Secret	Root Detections	Malware Check	Security Score
1	OVO	YES	YES	YES	NO	YES	GOOD	47
2	GoPay	YES	YES	NO	NO	YES	GOOD	49
3	Shopee Pay	YES	YES	YES	YES	YES	GOOD	17
4	DANA	YES	YES	NO	YES	YES	GOOD	12

Sumber: (Yudatama Arya, 2023)

Pada tabel 2 menjelaskan Analisis Peningkatan dan Penurunan Skor Keamanan yaitu:

1. OVO
    - Peningkatan kecil skor keamanan dari 47 menjadi 48 menunjukkan adanya perbaikan pada beberapa aspek keamanan, meskipun risiko seperti weak crypto, SSL bypass, dan dangerous permissions masih ditemukan.
    - Faktor penyebab peningkatan dapat mencakup pembaruan teknologi keamanan dan penerapan kebijakan lebih ketat terkait permissions.
2. GoPay

- Penurunan skor dari 49 menjadi 47 mengindikasikan bahwa beberapa aspek keamanan mungkin belum diperbarui atau mengalami pengurangan efektivitas.
- Faktor penurunan bisa disebabkan oleh kurangnya pembaruan keamanan atau munculnya kerentanan baru yang tidak tertangani dengan baik.

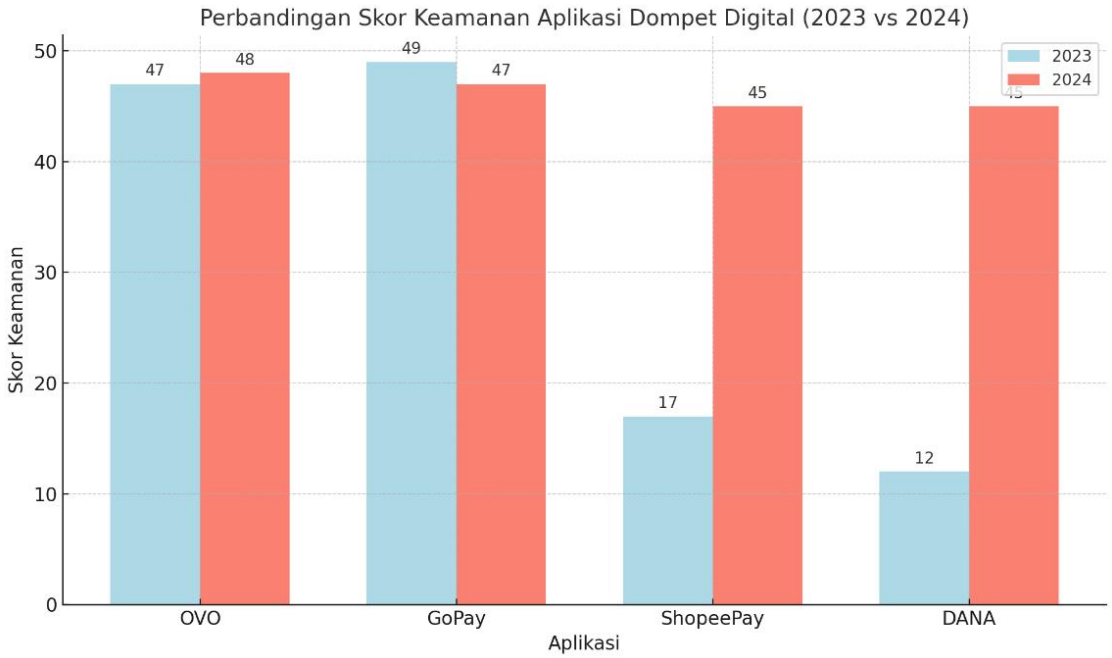
3. ShopeePay
    - Peningkatan besar dari skor 17 ke 45 menunjukkan bahwa ShopeePay melakukan perbaikan signifikan, termasuk mengurangi risiko hardcoded secret dan meningkatkan pengamanan terhadap dangerous permissions.
    - Faktor peningkatan ini kemungkinan besar berasal dari audit keamanan menyeluruh dan investasi dalam teknologi baru untuk pengamanan aplikasi.
4. DANA
    - Lonjakan skor dari 12 ke 45 mencerminkan usaha besar dalam meningkatkan keamanan aplikasi, terutama dalam menangani kelemahan seperti *hardcoded secret* dan *dangerous permissions*.
    - Faktor yang berkontribusi dapat mencakup integrasi teknologi enkripsi baru, pengurangan izin berisiko, serta peningkatan proses pengembangan aplikasi yang berfokus pada keamanan.

Tingkat Keamanan dari empat Aplikasi dompet digital yang dianalisis pada tahun 2023 adalah sebagai berikut :

1. OVO WhatsApp memiliki tingkat keamanan Tingkat 4 dan menjadi peringkat ke 2
2. Go Pay memiliki tingkat keamanan Tingkat 4 menjadi peringkat ke 1
3. DANA memiliki tingkat keamanan Tingkat 4. menjadi peringkat ke 4
4. Shopee Pay memiliki tingkat keamanan Tingkat 4 menjadi peringkat ke 3

Berdasarkan hasil analisis pada tahun 2024 dan perbandingannya dengan data tahun 2023, terdapat beberapa perubahan dalam skor keamanan (*security score*) pada aplikasi dompet digital yang dianalisis. Berikut adalah grafik perbandingan perubahan skor keamanan:

Gambar 2. Grafik perbandingan analisis statis



Sumber: Hasil Penelitian (2024)

Gambar 2. Grafik perbandingan analisis statis

Pada Gambar 2 menunjukan perbandingan skor keamanan aplikasi dompet digital antara tahun 2023 dan 2024 dalam bentuk grafik, yang mencakup empat aplikasi utama: OVO, GoPay, ShopeePay, dan DANA. Pada tahun 2023, OVO memiliki skor keamanan 47, yang meningkat menjadi 48 pada tahun 2024. Peningkatan ini tergolong kecil namun menunjukkan adanya perbaikan dalam beberapa aspek keamanan. Sebaliknya, GoPay mengalami penurunan skor dari 49 pada tahun 2023 menjadi 47 pada tahun 2024, menandakan adanya penurunan efektivitas pada beberapa parameter keamanan.

Sementara itu, ShopeePay mencatat peningkatan signifikan dari skor 17 pada tahun 2023 menjadi 45 pada tahun 2024, mencerminkan perbaikan besar dalam sistem keamanan, termasuk penanganan kerentanan yang lebih baik. Hal serupa juga terjadi pada DANA, yang menunjukkan peningkatan skor dari 12 pada tahun 2023 menjadi 45 pada tahun 2024, menggambarkan investasi besar dalam teknologi dan kebijakan keamanan. Secara keseluruhan, ShopeePay dan DANA memiliki peningkatan skor keamanan paling signifikan, sedangkan OVO hanya mengalami peningkatan kecil. Di sisi lain, penurunan skor GoPay menunjukkan perlunya perbaikan lebih lanjut untuk mempertahankan standar keamanannya.

4. Kesimpulan

Berdasarkan hasil analisis dan perbandingan tingkat keamanan pada empat aplikasi dompet digital di Indonesia, ditemukan dinamika yang mencerminkan perkembangan signifikan di sektor ini. ShopeePay dan DANA menunjukkan peningkatan yang sangat signifikan dalam

skor keamanan dibandingkan tahun sebelumnya. Peningkatan ini kemungkinan besar didorong oleh komitmen mereka untuk meningkatkan perlindungan data pengguna, termasuk melalui penerapan teknologi keamanan yang lebih baik dan audit yang menyeluruh terhadap aplikasi mereka.

Di sisi lain, OVO menunjukkan tingkat keamanan yang stabil dengan sedikit peningkatan skor dari 47 menjadi 48. Hal ini mengindikasikan bahwa meskipun langkah-langkah keamanan yang diterapkan cukup memadai, masih ada ruang untuk perbaikan, terutama pada aspek seperti enkripsi lemah dan bypass SSL. Komitmen OVO dalam menjaga keamanan platformnya tetap terlihat meskipun perubahan yang dilakukan tidak signifikan.

Sementara itu, GoPay mengalami penurunan skor keamanan dari 49 menjadi 47. Penurunan ini dapat mencerminkan tantangan dalam menjaga standar keamanan di tengah munculnya kerentanan baru. Hasil ini menunjukkan bahwa GoPay perlu meningkatkan upaya pengamanan, baik melalui pembaruan teknologi maupun kebijakan keamanan yang lebih ketat untuk mengurangi risiko yang mungkin dihadapi pengguna.

Secara keseluruhan, hasil penelitian ini menyoroti pentingnya pengembangan dan pembaruan berkelanjutan dalam aspek keamanan aplikasi dompet digital. Dengan tingkat keamanan yang berada pada level empat untuk semua aplikasi yang dianalisis, langkah-langkah perlindungan dasar telah terpenuhi. Namun, perbedaan skor keamanan menunjukkan bahwa masih ada aspek spesifik yang memerlukan perhatian lebih besar oleh masing-masing penyedia layanan. Keberlanjutan upaya ini akan sangat penting untuk memastikan kepercayaan pengguna, menjaga privasi data, dan mendukung pertumbuhan ekosistem fintech yang aman di Indonesia.

Daftar Pustaka

Firmansyah, P. D., Fauzi, A., Barja, R., Mulyana, A. P., Putri, T. N., Surachman, A., & Ramadhan, G. (2024). Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalisasi Perlindungan Data Dengan Teknologi Lanjutan. *Jurnal Kewirausahaan Dan Multi Talenta*, *2*(2), 112–125. https://siberpublisher.org/index.php/JKMT/article/view/160

Jelamu, M. S., Kiak, N. T., & Tiwu, M. I. H. (2024). Analisis Moderasi Inklusi Keuangan Aplikasi Financial Technology Terhadap Penggunaan Pinjaman Online Masyarakat Kota Kupang. *Jurnal Ilmiah Mahasiswa Perbankan Syariah (JIMPA)*, *4*(2), 705–722. https://doi.org/10.36908/jimpa.v4i2.431

Marginingsih, R. (2021). Financial Technology (Fintech) Dalam Inklusi Keuangan Nasional di Masa Pandemi Covid-19. *Moneter - Jurnal Akuntansi Dan Keuangan*, *8*(1), 56–64. https://doi.org/10.31294/moneter.v8i1.9903

Munir, M. M., & Hakim, M. N. (2024). Kepuasan Pengguna Melalui Kualitas Input Dan Output User Satisfaction Through the Quality of Input and Output of the Management Information System At Sma Negeri 1 Gondang. *JICN: Jurnal Intelek Dan Cendekiawan Nusantara*, *1*(4), 5049–5058.

Peraturan Bank Indonesia Nomor 19/12/PBI/2017. (2017). Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial. *Bank Indonesia*, 1. https://www.bi.go.id/id/sistem-pembayaran/fintech/Contents/default.aspx

Riset, J., Utomo, B. C., & Rahman, A. A. (2024). *Analisis Kesadaran Keamanan Data Pribadi pada Pengguna E-Wallet Analysis of Personal Data Security Awareness of DANA E-Wallet Users*. *8*(2), 155–166.

Rizkika, P., Juardi, D., & Susilo Yuda Irawan, A. (2024). Analisis Keamanan Pada Aplikasi Himfo Berbasis Android Menggunakan Mobsf. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(4), 5945–5952. https://doi.org/10.36040/jati.v8i4.10051

Sulomo, W. P. (2019). Tugas Sistem Informasi Manajemen: Keamanan Informasi Dalam Pemanfaatan Teknologi Informasi Pada PT. Bank Central Asia Tbk. *ResearchGate*, *November*, 1.

Wijayanto, H., Muhammad, A. H., & Hariyadi, D. (2020). Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid. *Jurnal Ilmiah SINUS*, *18*(1), 1. https://doi.org/10.30646/sinus.v18i1.433

Yasa, R. novita, & Nugraha, A. C. F. (2024). Perbandingan Keamanan Aplikasi Pesan Instan Android Menggunakan MobSF (Mobile Security Framework) Berdasarkan Beberapa Standar. *Info Kripto*, *18*(1), 9–14. https://doi.org/10.56706/ik.v18i1.88

Yudatama Arya, G. I. (2023). Analisis Keamanan Aplikasi Dompet Digital Pendekatan Statis dan Dinamis. *Jurnal Manajeman Informatika*, *17*(1), 18–22. https://www.sttrcepu.ac.id/jurnal/index.php/simetris/article/view/321